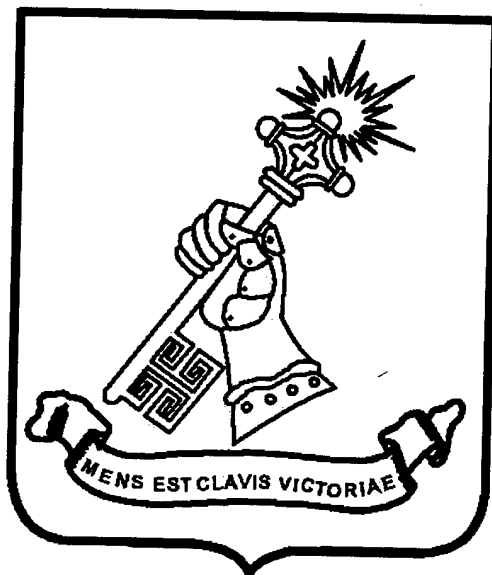


# **CREATING A DOD STRATEGIC INFORMATION SUPPORT CENTER**

**A MONOGRAPH**

**BY**

**Major Erin J. Gallogly-Staver  
Military Intelligence**



**School of Advanced Military Studies  
United States Army Command and General Staff College  
Fort Leavenworth, Kansas**

**Second Term AY 98-99**

Approved for Public Release Distribution is Unlimited

**DTIC QUALITY INSPECTED 4**

**19991109 041**

| REPORT DOCUMENTATION PAGE  |   |  | Form Approved<br>OMB No. 0704-0188             |                                  |
|--|---|--|--|----------------------------------|
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503. |   |  |  |                                  |
| 1. AGENCY USE ONLY (Leave blank)   |   | 2. REPORT DATE                                     |  | 3. REPORT TYPE AND DATES COVERED |
| 4. TITLE AND SUBTITLE<br>CREATING a DoD Strategic Information Support Center   |   |  | 5. FUNDING NUMBERS                             |                                  |
| 6. AUTHOR(S)<br>Erin J Gallogly-Staver   |   |  |  |                                  |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>SAMS<br>EH 274 1 REYNOLDS AVE<br>FLKS 66727  |   |  | 8. PERFORMING ORGANIZATION REPORT NUMBER       |                                  |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)<br>SAME AS 7   |   |  | 10. SPONSORING/MONITORING AGENCY REPORT NUMBER |                                  |
| 11. SUPPLEMENTARY NOTES  |   |  |  |                                  |
| 12a. DISTRIBUTION / AVAILABILITY STATEMENT<br><br>APPROVED FOR PUBLIC RELEASE:<br>DISTRIBUTION UNLIMITED.  |   |  | 12b. DISTRIBUTION CODE                         |                                  |
| 13. ABSTRACT (Maximum 200 words)<br><br>SEE ENCL   |   |  |  |                                  |
| 14. SUBJECT TERMS<br>INFORMATION OPERATIONS, INFORMATION WARFARE, PSYCHOLOGICAL OPERATIONS   |   |  | 15. NUMBER OF PAGES<br>50                      |                                  |
|  |   |  | 16. PRICE CODE                                 |                                  |
| 17. SECURITY CLASSIFICATION OF REPORT<br>UNCLASS   | 18. SECURITY CLASSIFICATION OF THIS PAGE<br>UNCLASS | 19. SECURITY CLASSIFICATION OF ABSTRACT<br>UNCLASS | 20. LIMITATION OF ABSTRACT<br>UNLIMITED        |                                  |

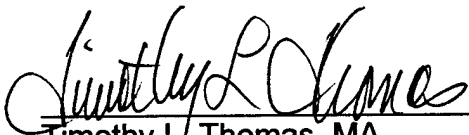
SCHOOL SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

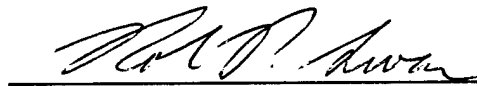
Major Erin J. Gallogly-Staver

Title of Monograph: *Creating a Department of Defense Strategic Information  
Support Center*

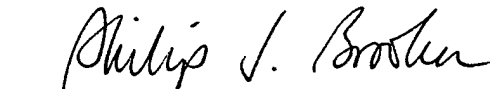
Approved by:

  
\_\_\_\_\_  
Timothy L. Thomas, MA

Monograph Director

  
\_\_\_\_\_  
LTC Robin P. Swan, MMAS

Director, School of Advanced  
Military Studies

  
\_\_\_\_\_  
Philip J. Brookes, Ph.D.

Director, Graduate Degree  
Program

Accepted this 27th Day of May 1999

## ABSTRACT

**CREATING A DEPARTMENT OF DEFENSE STRATEGIC INFORMATION SUPPORT CENTER** by MAJ Erin J. Gallogly-Staver, USA, 40 pages.

The U.S. Armed Forces needs a new organization capable of remaining competitive in an ever-expanding global information environment, adapting to reach both illiterate and technologically-savvy audiences of the 21<sup>st</sup> Century, developing information strategies to shape the global information environment, and responding to positive and negative information within the global information environment. The U.S. military must shed its Cold War organization, policy, doctrine, and equipment and prepare for the 21<sup>st</sup> Century. If the military fails to adapt, some other non-military organization may take its place. The new organization may have the expertise, but not the loyalty or deployability that a Department of Defense Strategic Information Support Center (D-SISC, pronounced DEE-SIK) could have.

Interagency coordination regarding information activities conducted by the military and other government organizations is episodic at best. Currently, there is no standing organization at the military strategic level to conduct interagency coordination and deconfliction between military and other governmental information activities.

In an environment of shrinking budgets, increased operational tempo, and continued downsizing, the U.S. Armed Forces must change to meet the needs of the 21<sup>st</sup> Century and *Joint Vision 2010*. Recent history demonstrates that the side with the ability to rapidly present its policy, strategy, and position to a variety of audiences in a coherent manner achieves an information advantage. A single organization, such as the DoD Strategic Information Support Center, from which military information activities can be coordinated, integrated, deconflicted, and synchronized is a step in the right direction.

## TABLE OF CONTENTS

|      |                                      |    |
|------|--------------------------------------|----|
| I.   | INTRODUCTION AND BACKGROUND.....     | 1  |
| II.  | CAPABILITIES REQUIRED.....           | 13 |
| III. | CURRENT CAPABILITIES AVAILABLE ..... | 21 |
| IV.  | CONCLUSIONS AND RECOMMENDATIONS..... | 30 |
|      | ENDNOTES .....                       | 41 |
|      | BIBLIOGRAPHY .....                   | 46 |

## **I: INTRODUCTION AND BACKGROUND**

Your leaders are not strategic thinkers. They said, "Let's bomb Yugoslavia and then figure out what to do next."<sup>1</sup>

Yugoslavia President Slobodan Milosevic

Current events support the hypothesis that the United States is losing the information war with Yugoslavia leader, Slobodan Milosevic. Dr. Kenneth Allard, a retired U.S. Army colonel and information warfare expert, comments that Yugoslav government ministers are "doing a better job getting on our air than we are getting on theirs. It clearly shows they understand the importance of an information campaign."<sup>2</sup>

At the end of April 1999, over six weeks into the Allied air operation, the state-run radio and television stations were still operational in Yugoslavia even though "NATO officials have insisted that propaganda—along with the special police—is one of Milosevic's two keys to power."<sup>3</sup> On the day prior to the start of the Allied air operation, the Yugoslav government shut down opposition radio and television stations and began to broadcast state-run programs over the opposition channels. Additionally, "Mr. Milosevic has expelled Western journalists and cut off television links" and his Information Ministry reviews the material broadcast by the few remaining reporters.<sup>4</sup> In Yugoslavia, government sources continue to proffer the story that the Kosovar Albanians "are not refugees because of us Serbs. They are running away from the bombs. The American propaganda is a complete setup."<sup>5</sup>

"Even Belgrade's antiwar propaganda is markedly Western. Billboards borrow Nike's slogan in urging NATO to 'Stop the Bombs. Just Do It.'"<sup>6</sup> According to Dr. Jacob Kipp, analyst at the U.S. Army's Foreign Military Studies Office, the Yugoslav

government has contracted Serbians, who work for Coca Cola, to help it with its information campaign.

While the United States has a robust informational element of power, recent experience demonstrates that the United States is unable to use this power to its advantage. The American media continues to question the efficacy of air operations without the credible threat of ground forces.<sup>7</sup> General Klaus Naumann, head of NATO's military committee, even commented, "So far in military history, we have not seen an operation which was successful by using air power exclusively."<sup>8</sup> Historian and author, John Keegan, describes the failure of "air control" throughout history from the British bombing of Iraq in 1920, through the strategic bombing campaign against Germany in World War Two, to Vietnam.<sup>9</sup> By day seven, the U.S. military was answering questions about its ability to maintain the bombing operation due to shortages of cruise-served missiles.<sup>10</sup> Former senator Sam Nunn argues, "We've got to find better tools, because when you really are trying to affect the hearts and minds of people—not conquer territory, not kick somebody out of a country, because this is their country—then you have an obligation to think through your strategy. . . . We should have been trying to turn the Serbian people against Milosevic before we started bombing."<sup>11</sup>

If the U.S. government and military are not satisfied with their current approach of "minimal resource investment for marginally effective strategic information programs," then some corrective action should be taken.<sup>12</sup> An alternative is to promulgate a national information strategy similar to the ones articulated in the Reagan/Bush-era National Security Strategy documents and create a Department of Defense Strategic Information Support Center.

## Historical Perspective

Interagency coordination regarding information activities conducted by the military and other government organizations is episodic at best. Currently, there is no standing organization at the military strategic level to conduct interagency coordination and deconfliction between military and other governmental information activities. Although there have been organizations in the past that were given the charter to oversee U.S. government information activities, they were undermanned, underfunded, and used marginally.<sup>13</sup>

Currently there is an ad hoc group, the International Public Information Core Group chaired by the State Department and composed of members of several government organizations involved in information activities, that meets to coordinate interagency information activities. Upon approval of the Presidential Decision Directive on International Public Information (PDD-IPI), the Core Group will "manage or oversee international public information activities. . . . and raise appropriate issues for Deputies' Committee-level decision."<sup>14</sup>

The following government documents and previous organizations establish policy and historical precedent for a DoD Strategic Information Support Center.

- National Security Decision Directive (NSDD) 130, *U.S. International Information Policy* (March 1984)<sup>15</sup>.
- 1985 and 1990 Psychological Operations Master Plans.
- State Department-War-Navy Coordinating Committee (SWNCC) (October 1946).



- National Security Council's Psychological Operations Coordinating Committee (March 1986).

- Several ad hoc National Security Council information management groups, such as the Sub-Group for International Information established to develop and coordinate the U.S. government information program during the initial stages of U.S. involvement in Bosnia.

A first step is for the U.S. Armed Forces to create an organization at the military-strategic level to integrate, coordinate, deconflict, and synchronize military information activities within the Department of Defense and with other government organizations conducting information activities. The majority of the capabilities required to establish a DoD Strategic Information Support Center exist within the U.S. Armed Forces; unfortunately, many of the organizations with complementary capabilities are competing with each other for limited resources. A joint center can leverage current capabilities and future technologies to gain efficiencies being lost by continued downsizing of the U.S. Armed Forces and deconflict competing agencies' efforts.

The proposed DoD Strategic Information Support Center, composed of military units and organizations that analyze, plan, or conduct strategic and operational information activities, would:

- develop information strategies to shape the global information environment in a way favorable to U.S. interests, policies, and strategies.

- provide a capability to respond to events that occur within the global information environment. For example, neutralize information that is in contravention and highlight information favorable to U.S. interests, policies, and strategies.

- coordinate DoD information policy with theater Commanders-in-Chief and with other government agencies;

- coordinate, integrate, deconflict, and synchronize all DoD information activities;

- coordinate, integrate, deconflict, and synchronize its information activities with other U.S. government organizations that conduct information activities.

If the DoD Strategic Information Support Center existed today, it would propose a military information strategy for actions in Kosovo to the ad hoc International Public Information Core Group. The Center would encourage other U.S. government organizations to develop information strategies that would support or at a minimum, not counter, the military information strategy. Further, it would coordinate all the military organizations and units, such as public affairs units, Service and Joint information warfare organizations, computer emergency response teams, and psychological operations units, involved in analyzing, planning for, and conducting information activities. The goal would be to have a coherent, well-thought out information strategy to counter Milosevic's disinformation campaign and help achieve U.S. and NATO objectives.

The planning worksheet (Figure 1) is a simple example of how the DoD Strategic Information Support Center would coordinate, integrate, deconflict, and synchronize military information activities. It would use similar tools to coordinate DoD's information strategy with those of other U.S. Government organizations' strategic information activities.

| <b>PHASE A: Description</b><br>(Projected Timeframe)   | <b>PHASE B: Description</b><br>(Projected Timeframe) | <b>PHASE C: Description</b><br>(Projected Timeframe) |
|--|--|--|
| 1. JPOC<br>2. video 1<br>3. disseminate on local TV<br>4. D+1<br>5. themes 1 & 2<br>6. USIS  | 1.<br>2.<br>3.<br>4.<br>5.<br>6.                     | 1.<br>2.<br>3.<br>4.<br>5.<br>6.                     |
| 1. Multi-Media & Combat Camera<br>2. still & video footage<br>3. document violations<br>4. D-5 – D-2<br>5. provide footage to JPOC<br>6. JPOC & Public Affairs | 1.<br>2.<br>3.<br>4.<br>5.<br>6.                     | 1.<br>2.<br>3.<br>4.<br>5.<br>6.                     |
| 1. Computer Support Activity<br>2. vulnerabilities assessment<br>3. computer defense ops<br>4. D-5 – D+2<br>5. prevent interference<br>6. JPOC, MM&CC          | 1.<br>2.<br>3.<br>4.<br>5.<br>6.                     | 1.<br>2.<br>3.<br>4.<br>5.<br>6.                     |
| 1. Joint IO Support Center<br>2. assessment report<br>3. assess affects<br>4. D+2-D+10<br>5. assess<br>6. JPOC, USIS   | 1.<br>2.<br>3.<br>4.<br>5.<br>6.                     | 1.<br>2.<br>3.<br>4.<br>5.<br>6.                     |
| <b>1=Organization, 2=Product, 3=Action Taken, 4=Timeframe, 5=Purpose, 6=Coordination Affected Comments</b>   |  |  |

Figure 1. Example Planning Worksheet

### Definitions

This monograph uses the following definitions compiled from numerous interviews with serving and retired government officials. **Strategic information** includes all information activities conducted by the U.S. Government to achieve its national security objectives. **Information activities** include international public information, special information activities, technical information operations, and Department of Defense information operations. **International public information**

includes public affairs, public diplomacy, and international military information, formerly called strategic psychological operations, designed to affect foreign audiences in ways favorable to U.S. interests. "The term 'international military information' is a U.S. government interagency-approved term for describing what used to be known as 'strategic psychological operations'."<sup>16</sup> Whenever Department of Defense psychological operations are supporting a U.S. government-led strategic information activity, the term psychological operations will be replaced with international military information.

**Special information activities** are National Security Council-led compartmented Department of Defense psychological operations, also known as the Overt Peacetime Psychological Operations Program (OP3). **Technical information operations** are National Security Council-led compartmented information operations conducted by government organizations, such as the Central Intelligence Agency, National Security Agency, Department of Justice, or Department of Commerce. **Department of Defense information operations** are actions taken to affect adversary information and information systems while defending one's own information and information systems. Capabilities and activities used to conduct DoD information operations include operations security, psychological operations, military deception, electronic warfare, physical destruction, computer network attack and defend, public affairs, and civil affairs.<sup>17</sup> Most DoD information operations are conducted at the operational or tactical level. However, planners of DoD information operations should coordinate, integrate, and deconflict operations with planners of strategic information activities. Figure 2 graphically depicts the relationship among these terms.

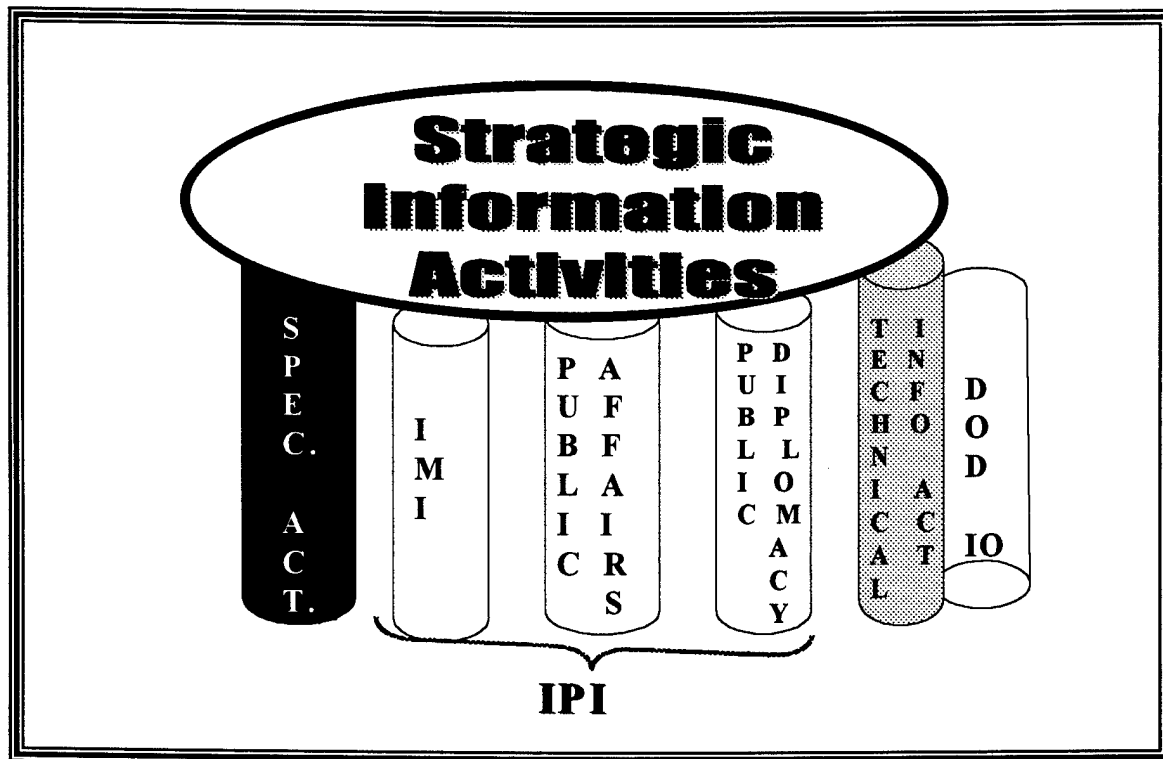


Figure 2. Terms of Reference

### Evaluation Criteria

This monograph uses several evaluation criteria to evaluate how a DoD Strategic Information Support Center can meet the needs of the Armed Forces in the 21<sup>st</sup> Century. The criteria seek to evaluate whether the Center enables the U.S. Armed Forces to shape, prepare, and respond to and within the environment envisioned in *Joint Vision 2010*. These criteria are integration, speed, flexibility, and synergy.

**Joint/Interagency integration** is defined as an organization in which elements of more than one Service participates and conducts liaison with other organizations of the U.S. Government. This concept extends even to leadership skills, where “the dynamic nature of joint operations in the 21<sup>st</sup> Century battlespace will require a continued emphasis on developing strong leadership skills . . . and the continuing refinement of

force structure and organizations (that) will require leaders with a knowledge of the capabilities of all four services.”<sup>18</sup>

**Speed** is defined as “less ‘startup’ time between deployment and employment”<sup>19</sup> than the current organizational structure allows. Currently, innumerable Joint and Service organizations, such as the Joint Command and Control Warfare Center (JC2WC), the Land Information Warfare Activity (LIWA), 4<sup>th</sup> Psychological Operations Group, 193d Special Operations Squadron, and public affairs units in the Reserve Component, augment an ad hoc organization formed to provide strategic information support at the military strategic level. At the operational and tactical levels, these same organizations deploy elements to a theater Commander-in-Chief’s or Commander, Joint Task Force’s staff and component commands. While all these organizations plan and/or conduct information activities, there are currently no formal procedures by which to coordinate, integrate, deconflict, or synchronize their operations. “This continued ad hoc approach to coordinating, integrating, deconflicting, and synchronizing US Government strategic information has adversely impacted *timely*, accurate, and effective informational activities conducted in Bosnia over the long-term.”<sup>20</sup>

**Organizational flexibility** is defined as the ability to offer numerous and multi-functional force packages to meet the informational needs of the supported commander. For example, a force package comprised of analysts, planners, support personnel, and operators who can plan for and conduct psychological operations, public affairs, and computer network defense.

A new organization must demonstrate **synergy**. Its value added must be greater than the sum value added of its component parts. It must be capable of remaining

competitive in and adapting to an ever-changing global information environment and in the face of decreasing military budgets.

### **Assumptions**

This monograph makes five assumptions. First, that the manpower allocated to current information organizations are sufficient to create a DoD Strategic Information Support Center. Second, that current policy and legal restrictions will be modified to meet 21<sup>st</sup> Century requirements. For example, there are no acquisition constraints prohibiting purchase of and modification to off-the-shelf equipment for military use. Third, current Service parochialism will concede to the spirit of jointness promulgated in *Joint Vision 2010*. Fourth, the Presidential Decision Directive on International Public Information (PDD-IPI) is approved. Lastly, Cold War Reserve Component activation procedures will be revised to meet time-sensitive requirements of the 21<sup>st</sup> Century.<sup>21</sup>

### **The New Global Information Environment**

The authority and control of traditional Westphalian nation-states continue to wane in the current information-age. Non-nation state actors, such as multi-national corporations, global nongovernmental organizations, and terrorist, drug, and organized crime organizations, continue to grasp more power traditionally associated with nation-states. The elements of national power—diplomatic/political, economic, military, social/cultural, and informational—are no longer the sole purview of recognized nation-states. With commercially-available technology, such as space-based communications, and the near-instantaneous availability of information, non-nation-state actors have increasingly more power. (See Figure 3.) Witness the power Osama Bin Laden, the Saudi millionaire and terrorist, demonstrated recently against the United States. The

Department of State links Bin Laden to the U.S. Embassy bombings in Kenya and Tanzania in 1998. Subsequent to the bombings, the United States launched cruise missile attacks against Bin Laden's headquarters in Afghanistan and a factory in Sudan. The United States claimed the factory was used to produce weapons; Sudanese authorities claimed the factory produced medicine.<sup>22</sup> Similarly, Somalia warlord, Mohamed Farrah Aidid, used his technological inferiority to his advantage against superior U.S. forces. The result? U.S. forces withdrew from Somalia after eighteen servicemen were killed and the body of a serviceman was drug through the streets of Mogadishu. Did Aidid have a comprehensive information strategy to discredit U.S. forces or was it sheer luck? The U.S. government and the Armed Forces must adjust their policies, strategies, organizational structures, and processes to remain relevant and to effectively deal with the new global information environment.

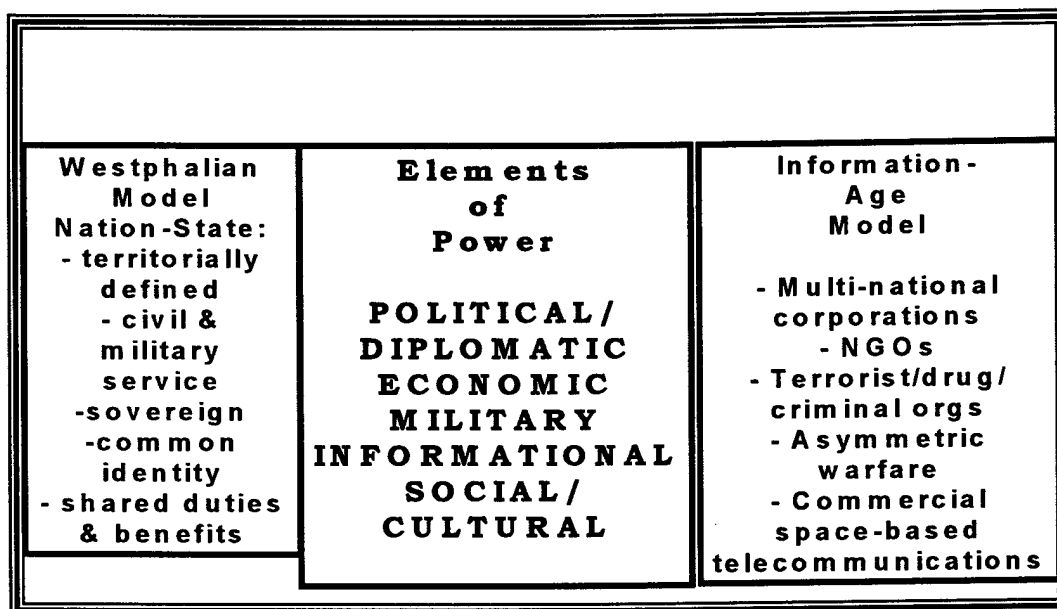


Figure 3. New Global Information Environment



## **Threats in the 21<sup>st</sup> Century**

According to Major General Robert Noonan, Commanding General, U.S. Army Intelligence and Security Command, the United States will face three distinct types of threats: peer competitor, asymmetrical regional hegemons, and warriors. China, Russia, and Japan are the likely peer competitors by 2016. North Korea, Iraq, and Iran are three countries in which a regional conflict is likely. Warrior threats are those true believers or opportunist who will ignore laws, exploit chaos, and have little to lose relative to their enemies.<sup>23</sup> Terrorist organizations, insurgent forces, or drug and criminal organizations describe a warrior threat. These adaptive threats will have access to commercially-available technology, such as Iridium, encryption, and imagery, and technology available from black markets, such as sophisticated weapons systems and their associated technology. As demonstrated by operations in Kosovo, Belgrade-based hackers ping NATO computer systems and "may move on to more damaging activities such as downloading press releases and overhead imagery available on the (NATO) site, tampering with them, and then releasing them as official policy."<sup>24</sup> These threats are unlike any threat previously encountered; they will study U.S. strengths and weaknesses and attempt to attack the United States in ways for which it is ill-suited to respond or react.

## II: CAPABILITIES REQUIRED

We're quite sure that we only hit military vehicles. . . . the next day NATO spokesman Jamie Shea acknowledged that the pilot made a mistake.<sup>25</sup>  
USIA and NATO

"To retain our effectiveness with less redundancy, we will need to wring every ounce of capability from every available source. That outcome can only be accomplished through a more seamless integration of Service capability. To achieve this integration while conducting military operations we must be fully joint: institutionally, organizationally, intellectually, and technically."<sup>26</sup> A DoD Strategic Information Support Center can enable this mandate set forth in *Joint Vision 2010*.

The capabilities required for a DoD Strategic Information Support Center are multi-dimensional and are not present in *any one single* organization in today's Armed Forces. However, the capabilities required exist within the Armed Forces; Chapter III provides information on units currently available in the inventory. This chapter provides a brief description of the required capabilities.

### Collection

The DoD Strategic Information Support Center would require two types of collection: traditional intelligence collection and pre-production collection. Traditional intelligence collection includes basic and current intelligence. Analysts collect basic and current intelligence in open-source or unclassified sources, such as the Internet or literary journals, and classified sources, such as Intelink.

Basic intelligence includes historical reports, longitudinal studies, archival records, academic research, and official transcripts. A multitude of government and academic institutions collect, evaluate, collate, and disseminate basic intelligence

information. For example, the Central Intelligence Agency publishes biographical sketches; the U.S. Information Agency conducts extensive studies on foreign media and audiences. Academic institutions have volumes of data on foreign cultures, demographics, histories of virtually every ethnic group, tribe, or otherwise cohesive group, and infrastructure. International organizations also collect information on the culture, infrastructure, and geography of countries in which they operate. The Center for Army Lessons Learned (CALL) is creating an organization, the University After Next (UAN), which attempts to leverage academic and other institutions to the benefit of the U.S. Army.

Current intelligence is used to update basic intelligence. Analysts procure current intelligence from some of the same sources used to extract basic intelligence, for example, the Defense Intelligence Agency or the Joint Command and Control Warfare Center. Planners need both types of intelligence from classified and open sources to plan, execute, and evaluate information policies, strategies, and campaigns.

Unlike order of battle intelligence required by general purpose military forces, planners developing information policies, strategies, and campaigns require people-oriented intelligence. For example, an infantry division primarily wants to know the strength, capabilities, composition, and disposition of the enemy unit it is facing; whereas, information planners need intelligence on a target's leadership, decision-making process, and communication's architecture to include hardware, software, and firmware. They need to know what factors compose the "will" of the target audience.

Pre-production collection includes materials used to produce products. Video footage, still photographs, newspaper articles, and interviews are examples of input used

to produce products. The Desert Storm psychological operations video, "Nations of the World Draw a Line in the Sand," disseminated throughout the western world and smuggled into Iraq used video footage provided by the Joint Combat Camera Center and several Service public affairs organizations. The DoD Strategic Information Support Center must also have an archival system that can systematically warehouse high volumes of data and imagery and retrieve that data for developing multi-media products in near real-time.

### **Analysis**

DoD Strategic Information Support Center analysts conduct analysis based on collection capabilities of the global information environment to determine potential problem areas that information activities could deter, contain, or otherwise influence to best serve U.S. national interests. Analysts also evaluate on-going information policies, strategies, and campaigns to determine their effectiveness. The capabilities required of a strategic analyst are more complex than those required for a general purpose military analyst. The strategic analyst must be well-versed in systems theory and complexity theory. Most important of all, he must understand the linguistic and cultural nuances of target audiences and the subtleties of U.S. foreign policy and their relationship to U.S. information strategies rather than strictly the capabilities of a weapon system. For example, analysts must be familiar with the format, content, and layout of the diverse products available within cultures. They will use this information to assist personnel produce products, such as television commercials and newspapers, to which a target audience would be receptive.

Technical analysts will be required to assess the communication's architecture of target audiences to determine ways to input information into the system and remove information to determine success of the information campaign. This diverse group of analysts will require access to highly-classified policies and plans and access to national level decision-makers.

### **Production**

The DoD Strategic Information Support Center will require a wide variety of production assets both on-hand and available at a short notice for world-wide employment. It must be capable of addressing innumerable targets over every medium to include print, audio, visual, digital, and virtual. Some production facilities, such as print plants, television studios, or computer centers may lend themselves to out-sourcing and government contracts. The Center must maintain some organic assets that are deployable and are capable of operating in austere environments. Operators must be proficient in the latest technology within their production genre in order to compete within the new global information environment. Technicians must also be available for deployment on short notice. It may not be feasible to recruit and retain certain highly-technical experts in the Armed Forces. However, the Center could ensure those capabilities are available either through contracts or experts on retainer. Recent experience in Bosnia demonstrated that the U.S. military lacked expertise required to produce television spots; fortunately, television producers and master camera operators were available through a government contract.<sup>27</sup>

Units deployed forward should also have a reach-back capability to send draft products between the forward-deployed location and home station. Current technology

exists to facilitate reach-back operations. Satellite time required to support reach-back operations is expensive. Several different Department of Defense organizations, such as the Armed Forces Radio and Television Service, the intelligence community, and the combat camera centers, are buying satellite time for their missions. The time has come for pooling resources and buying large Department of Defense blocks of satellite time, five to seven years into the future, to save money. The Department of Defense Strategic Information Support Center, in coordination with the Defense Information Support Agency, could play a significant role in centralizing requirements for satellite time, especially during a crisis when urgent priorities must be accommodated.

### **Dissemination**

The requirements for dissemination are similar to those required for production. The DoD Strategic Information Support Center will require both organic and out-sourced dissemination platforms. Dissemination platforms must run the gamut of today's commercially-available equipment to include manned and unmanned aircraft, radios, televisions, computers, holograms, balloons, and people. An operator's imagination and the target audience's communications architecture should be the only limits on dissemination platforms. The platforms must be rapidly deployable and capable of operating in austere conditions under both permissive and non-permissive, hostile environments.

### **Simulation**

The Center must have a simulation capability to conduct nodal analysis, conduct pre-tests of its products, and integrate its planning process. Analysts would analyze the target audience in a systematic way to determine its weaknesses and vulnerabilities to

strategic information activities. For example, the target audience may be the leaders of a country that are trying to produce weapons of mass destruction. A simulation would conduct a nodal analysis to determine how the country would produce a weapon of mass destruction. The country may need technical expertise and materiel from outside suppliers. It would construct facilities with known characteristics to conduct research, development, acquisition, and testing of the weapon system and its associated precursor materiel. The simulation may determine that the best way to negate the target audience's plans is to influence the supplier of a precursor material, such as high-grade steel used to build a testing facility. Similarly, a simulation could analyze the target audience's communications architecture to determine vulnerabilities to strategic information activities. Finally, a simulation could assist planners in the pre-test phase of analysis and in developing and assessing an information campaign within the planning process. For example, a pre-test conducted in the target audience's location could be broadcast live using a reach-back capability. Analysts would receive immediate feedback that could be used to modify products and assess an information campaign. These simulations would be similar to models and simulations currently used by a variety of military organizations.

### **Command and Control**

The command and control structure for the DoD Strategic Information Support Center must be robust and capable of operating in a variety of physical, political, and cultural environments simultaneously. The Center should be located in the vicinity of the Military District of Washington to facilitate coordination with senior military leaders and to participate in the interagency process. The base at which it is located should have sufficient communications architecture to support a variety of both unclassified and

classified global communications, such as video teleconferencing and satellite communications facilities.

The headquarters should be joint with rotating director and deputy director from the Services providing the majority of assets. For example, if U.S. Army and U.S. Air Force personnel fill the majority of the positions within the organization, then an Army and Air Force officer should rotate between director and deputy director.

Like any military organization, the Center should have a staff commensurate with its size to provide normal administrative and logistical functions. However, the staff should seek to leverage technology in an attempt to downsize bureaucratic overhead. Some expertise not germane to daily operations may lend itself to contracts and outsourcing. The Center should seek training with industry for its personnel to help keep them abreast of current technologies and commercial standards. This training would complement formal training military members receive within the military training system.

The plans and operations sections should be staffed with senior individuals with persuasive communications experience. These staff officers must be technically proficient and culturally savvy in multiple genres. For example, a planner may have served previously as a psychological operations officer and received training with industry in television production and desktop publishing. Another planner may have public affairs expertise and experience with Armed Forces Radio and Television Service. Yet another planner may be a Foreign Area Officer with expertise on the National Security Council staff. The key to the planning and operations sections will be their



breadth and depth of experiences in persuasive communications, current technology, and foreign cultures.

There should be senior liaison officers stationed with major information providers, such as the Department of State, United States Information Agency, Central Intelligence Agency, and the National Security Agency. Similarly, liaison officers from the DoD Strategic Information Support Center should co-locate with the theater Commanders-in-Chief to assist them with their Theater Information Campaigns. Finally, liaison officers may be required at other government organizations, such as the Congressional Liaison Office, the Federal Bureau of Investigation, the Department of Commerce, and the Drug Enforcement Agency, as the situation dictates.

### **Linguists**

Critical in today's multi-lingual global information environment is the requirement for highly-proficient linguists. The DoD Strategic Information Support Center must be able to support all of the Center's operations. It would use linguists to collect and analyze information, and produce and evaluate products in foreign languages, and provide interpretation support to the Center. Although a pool of trained linguists are needed to plan and execute information activities, some linguist support may offer itself to experts on retainer. Contracts for translation could be let or linguists at universities could be kept on retainer for languages used infrequently.

### **III: CURRENT CAPABILITIES AVAILABLE**

Ultimately, the effectiveness of the Iraqi propaganda effort reached even the White House. Without realizing it, the president, too, succumbed to those images of suffering Iraqis when he called off the (1998) U.S. attack.<sup>28</sup>

Ralph Peters

The organizations described below provide the majority of information support to or conduct of information activities for the Services and regional Commanders-in-Chief. Other generic organizations, such as maintenance and communications units, can provide support requirements that are not unique to the DoD Strategic Information Support Center.

#### **Joint and Service Information Warfare Organizations**

Currently, the Army, Navy, and Air Force all have an information warfare organization designed to provide information operations, information warfare, and command and control warfare support to the Service component commander and other Service organizations. These information organizations have similar capabilities—analysis of adversary signals, computer network defense functions, electronic warfare, and planning. Each organization's mission and capability are highlighted below.

##### **Joint Command and Control Warfare Center**

The Joint Command and Control Warfare Center, a subunified command of U.S. Atlantic Command (USACOM), provides information operations support to "unified commands, joint task forces, functional and service components, and subordinate combat commander . . . (and to the) Office of the Secretary of Defense, the Joint Staff, the services, and other government agencies."<sup>29</sup> The Center provides full spectrum information operations support to include Commander-in-Chief support teams,

wargaming and simulations, Red Team, exercise support, vulnerability assessment, doctrine and joint tactics, techniques, and procedures, and maintenance of numerous databases. The support teams “provide a pool of expertise that the Commanders-in-Chief can call upon to help with planning, course of action development, (and) targeting options . . . . (They) also augment the special technical operations (STO) personnel found in the joint force headquarters for integration and deconfliction of compartmented and non-compartmented requirements.”<sup>30</sup> The Center also has several electronic warfare simulations that planners use to plan for and evaluate information operations.

#### Land Information Warfare Activity

The Land Information Warfare Activity (LIWA), a field operating agency of the Department of the Army under the command of the U.S. Army Intelligence and Security Command (INSCOM), provides information operations, information warfare, and command and control warfare support to land component and separate Army commands. It also conducts liaison with other Service and Joint information warfare centers to develop and sustain interoperability.

Its mission is to “provide operational information warfare and command and control warfare support . . . to facilitate the planning and execution of information operations.”<sup>31</sup> The Land Information Warfare Activity provides Field Support Teams (FST) to assist Army commanders plan for C2 attack, C2 protect, and battlefield deception. Subject matter experts from command and control warfare disciplines—psychological operations, deception, operations security, electronic warfare, and physical destruction—comprise the multi-discipline teams that have access to national-level intelligence databases.<sup>32</sup> The Land Information Warfare Activity also operates the Army

Computer Emergency Response Team (ACERT) Central and the Army Reprogramming Analysis Team-Threat Analysis (ARAT-TA).

The ACERT coordinates C2 protect actions and responds to intrusions. Regional Army CERTs located at Eighth U.S. Army in Korea, U.S. Army Pacific (USARPAC) in Hawaii, and a continental United States CERT at Fort Huachuca, Arizona comprise the ACERT Central. These regional CERTs are co-located with network operations centers (NOCs) that are responsible for operating and maintaining the communications architecture. Major Pat Scribner, Field Support Team Leader at LIWA, uses a plumbing analogy to describe the relationship between the CERTs and NOCs: "The NOCs are like plumbers who lay and maintain the pipes. The signalers fix the pipes and are not concerned about the loss (of information). The CERTs look at loss of water and sewage (information) and where the pipes are broken."<sup>33</sup> The ACERT Central operates in concert with the other Service Computer Emergency and Intrusion Response Teams.

The ARAT-TA, in support of commanders and combat/materiel developers, identifies and reports changes in worldwide signature information that may require the rapid reprogramming of Army target sensing systems.<sup>34</sup> The ARAT-TA is co-located with the 68<sup>th</sup> Tactical Support Squadron at Eglin Air Force Base, Florida. The U.S. Air Force conducts the majority of signature analysis and reprogramming of all the Services.

The Director, LIWA is also the Commander, Army Forces (ARFOR) of the newly created Joint Task Force-Computer Network Defense (JTF-CND) at Space Command (SPACECOM). Space Command is the joint proponent for computer network defense. It remains to be seen how this new charter will affect organizations currently tasked to conduct computer network defense functions.

As currently organized, the Land Information Warfare Activity has 281 personnel. It is pending an increase to 300 in fiscal year 2000: 125 military, 86 government employees, and approximately 89 government contractors.

#### Fleet Information Warfare Center

The Fleet Information Warfare Center (FIWC), a subordinate command of Atlantic Fleet (CINCLANTFLT), provides information operations, information warfare, and command and control warfare support to the U.S. Navy. Their primary focus is on computer network defense and electronic warfare. The FIWC provides fleet augmentation to the Carrier Battle Groups (CVBG) and Amphibious Ready Groups (ARG). Currently, only the CVBGs have an Information Operations Commander who works with the intelligence and operations staff for situation development, planning, and execution. The Commander has no operational assets, but may exercise tactical control of any forces assigned to conduct information operations, information warfare, or command and control warfare.<sup>35</sup>

FIWC's computer network defense program is composed of three activities: vulnerability analysis and assistance, intrusion detection system monitoring, and Red Team. These C2 protect activities are designed to determine vulnerabilities, identify intrusions into information systems, raise awareness, and provide training. The Naval Computer Incident Response Team (NAVCIRT) is the Navy's central reporting point for all intrusion incidents; it also coordinates with the other Services' computer emergency response teams and other government agencies.

The FIWC also maintains electronic warfare databases and conducts reprogramming of target sensing systems after identification of changes in signatures.

This is the same function performed by the LIWA's ARAT-TA and the Air Force's 68<sup>th</sup> Tactical Support Squadron.

The U.S. Navy has radio broadcast equipment that deployed to Bosnia in support of Operation Joint Endeavor. These assets are available for tasking, but they have limited production and broadcast capabilities compared to Air National Guard and U.S. Army information operations assets, such as the EC-130E, Commando Solo, and the Transportable AM Transmitter-10kw (TAMT-10).<sup>36</sup> The Navy is considering contracting out for this capability for its ship and shore forces.

#### Air Force Information Warfare Center

The Air Force Information Warfare Center (AFIWC) develops, maintains, and deploys information operations, information warfare, and command and control warfare capabilities to Air Force major commands. The 1,000 military and civilian personnel at AFIWC perform five functions: operations support, database maintenance, modeling and analysis, engineering analysis, and mission support. "It provides technical expertise for computer and communications security and is the Air Force's focal point for tactical deception and operations security training. The AFWIC also organizes, trains, equips and deploys teams; develops and maintains databases and applications; performs vulnerability analysis of (U.S.) electronic systems; and protects (U.S.) command and control against adversary attacks."<sup>37</sup>

The AFWIC also includes the Air Force Computer Emergency Response Teams (AFCERTs) that provide "real-time operational network intrusion detection and perimeter defense (and) . . . coordinates the AFWIC's technical resources to assess,

analyze, and provide countermeasures for computer security incidents and vulnerabilities.”<sup>38</sup>

The Center also has several command and control warfare/information warfare models and simulations used by warfighters and the testing and acquisition communities. The models are generally used in the electronic warfare and communications security fields.

### **Other Information-Type Organizations**

The Armed Forces have a multitude of organizations that plan for, conduct, analyze, and/or support information operations. The units described below are the major units involved in information activities.

#### **Deception and Operations Security**

The Service information warfare organizations provide deception planning support to Service Component and separate Service commands, whereas the Joint Command and Control Warfare Center (JC2WC) provides deception planning support to joint forces. However, there are several special planning staffs and units with deception planning expertise that could support information activities conducted by the Department of Defense.<sup>39</sup>

#### **Electronic Warfare**

Each of the Service information warfare organizations and the Joint Command and Control Warfare Center have electronic warfare capabilities. These organizations coordinate with tactical and operational units that conduct electronic warfare to deconflict operations and synchronize the Joint Restricted Frequency List.

## Psychological Operations

All military psychological operations capabilities are in the U.S. Army save the EC-130E Commando Solo, an airborne dissemination platform, located in the Air National Guard. Approximately eighty percent of psychological operations units are in the Reserve Component; the 2d and 7<sup>th</sup> Psychological Operations Groups comprise the Reserve Component structure. The 4<sup>th</sup> Psychological Operations Group (Airborne) located at Fort Bragg, NC is the only Active Component psychological operations unit. As such, this unit is a strategic asset which supports U.S. national objectives worldwide and is the military's only information operations asset dedicated to psychological operations. Although the majority of operations conducted by the Group fall within the tactical to operational levels, the impact of their operations are often felt at the strategic and national levels. During Operation Uphold Democracy in Haiti, the Central Intelligence Agency airdropped thousands of transistor radios five days prior to the intervention so Haitians could listen to broadcasts conducted by Commando Solo.<sup>40</sup> Here, a national information asset, the Central Intelligence Agency, and a military information asset, the 4<sup>th</sup> Psychological Operations Group, worked closely to conduct successful operations. Perhaps the emerging integration of psychological operations' military assets and other informational assets at the national level will cause a relook into the creation of a Joint Psychological Operations Center discussed in the Secretary of Defense approved 1985 *Psychological Operations Master Plan*.<sup>41</sup>

## Information Operations

The Air Force's 690<sup>th</sup> Information Operations Squadron operates an Information Operations Center that integrates and conducts information operations. The Center



provides worldwide situation awareness by coordinating with national and theater intelligence centers, providing "Operations Reachback" services to deployed forces, and develops information warfare indications and warning for the Department of Defense. Their "CYBERWATCH" program maintains databases of foreign information warfare incidents based on the Defense Intelligence Agency's warning indicators, identifies foreign doctrine, capabilities, and intentions in the area of information warfare, and correlates the Defense Information Systems Agency (DISA) and Service CERTs data.<sup>42</sup>

#### Combat Camera and Visual Information Support

Each Service has its own combat camera (COMCAM) unit and there is a Joint Combat Camera Center (JCCC) that is "the central reception center for all Department of Defense combat camera still and video imagery."<sup>43</sup> Joint and Service combat camera units deploy visual information teams to collect and document Department of Defense operations and exercises, provide support to public affairs and information operations, assist in the development of situational awareness, and conduct surveillance and reconnaissance and battle damage assessment. The Joint and Service combat camera units, composed of both Active and Reserve Component servicemembers, have a variety of still and video capabilities.

Under Department of Defense Directive 5040.4, Joint Combat Camera Program, the Service combat camera units forward all still and video imagery to the Joint Combat Camera Center. The Center then catalogs and archives the material for approximately one year. It then transfers the footage to the Defense Visual Information Center (DVIC), the Department of Defense's central repository for images, where it is stored and safeguarded for approximately ten years at March Air Reserve Base, California. The

Center is currently preparing to put its archived collection on the Internet; the products will be available to all Department of Defense customers for use in visual information products. For example, public affairs officials use the footage collected by the combat camera team currently deployed to operations in Bosnia in national level briefings. Similarly, the psychological operations community uses footage obtained by the combat camera units in psychological operations products. Although the Joint Combat Camera Center falls under the Office of the Assistant Secretary of Defense for Public Affairs (OASD-PA), organizations outside the purview of the public affairs community use its products.

#### Linguists

The 300<sup>th</sup> Military Intelligence Brigade, Utah Army National Guard, provides linguist support to the Intelligence and Security Command (INSCOM), Department of the Army, theater Commanders-in-Chief, and the Department of Defense. They can provide intelligence production support, translation, and interpretation support in over thirty languages. Five-soldier teams comprised of officers, warrant officers, and enlisted soldiers with a variety of language-based intelligence military occupational specialties (MOSs) are capable of worldwide deployment. The Brigade has a Special Compartmented Information Facility (SCIF) that has a variety of communications means over which to transfer intelligence products or provide language support.

Although there are several small detachments in the Army Reserve with language skills, the 300<sup>th</sup> Military Intelligence Brigade is the only language unit with significant collection, analysis, production, and dissemination capabilities.

#### **IV: CONCLUSIONS and RECOMMENDATIONS**

Nothing is more dangerous in wartime than to live in the temperamental atmosphere of a Gallup Poll, always feeling one's pulse and taking one's temperature.<sup>44</sup>

Winston Churchill

Of the five elements of national power—diplomatic/political, economic, social/cultural, military, and informational—the informational element of power is the only element without an articulated strategy. The United States has a national military strategy, a foreign policy articulated by Department of State representatives and documents, and economic policies promulgated by the Council of Economic Advisors. The informational element, however, exists across all elements of power and has no one organization as its proponent. The United States Information Agency (USIA) provides information about U.S. foreign policy, institutions, and way of life to foreign audiences, but it does not have authority over other government organizations that conduct information activities. The same holds true for the military. Currently no one military organization has the charter to oversee military information activities.

##### **Military Information Activities: Proponents, Policy, & Doctrine**

Space Command (USSPACECOM) has responsibility for the newly formed Joint Task Force-Computer Network Defense. Special Operations Command (USSOCOM) has responsibility for psychological operations. Three different Assistant Secretaries of Defense (ASD) are proponents for different military information activities: psychological operations under ASD-Special Operations and Low Intensity Conflict (ASD-SOLIC), public affairs under ASD-Public Affairs (ASD-PA), and information operations under ASD-Command, Control, Communications, and Intelligence (ASD-C3I). Similarly, there is at least one Department of Defense Directive (DoDD) for each information

activity.<sup>45</sup> Unfortunately, none of these Directives is tied into a coherent policy or strategy. The Department of Defense should promulgate an overarching Directive that addresses military strategic and operational information activities. From this document, Chairman of the Joint Chiefs of Staff Instructions (CJCSI) and doctrinal manuals could articulate military policy and doctrine.

### **Organizational Structure**

Figure 3 depicts a recommended Department of Defense organization, the DoD Strategic Information Support Center (DoD-SISC pronounced DEE-SIK), for planning and conducting military strategic and operational information activities. This new center leverages technology, streamlines bureaucracies, eliminates mission redundancies, and seeks to integrate the efforts of various Department of Defense organizations. This new organization would not require any addition to the current force structure. It may, however, facilitate cuts in organizational staffing requirements due to the synergy gained by complementing capabilities.

### **Mission and Functions**

The Department of Defense Strategic Information Support Center would provide an integrated strategic information support function. It would coordinate, integrate, deconflict, and synchronize the operations of DoD organizations which conduct strategic and operational level information activities. Several current organizations would provide a few manpower billets to establish this integrated center. For example, the U.S. Army Civil Affairs and Psychological Operations Command (USACAPOC) headquartered at Fort Bragg, NC would provide the one-star deputy commander billet; the Active Component, such as U.S. Atlantic Command (USACOM) or U.S. Special Operations

Command (USSOCOM), would provide the two-star commander billet. This two-star billet would rotate among the Services that provide organizations to the DoD Strategic Information Support Center. Eventually there would be a formal Joint Manning Document based on the requirements set forth in *Joint Vision 2010*.

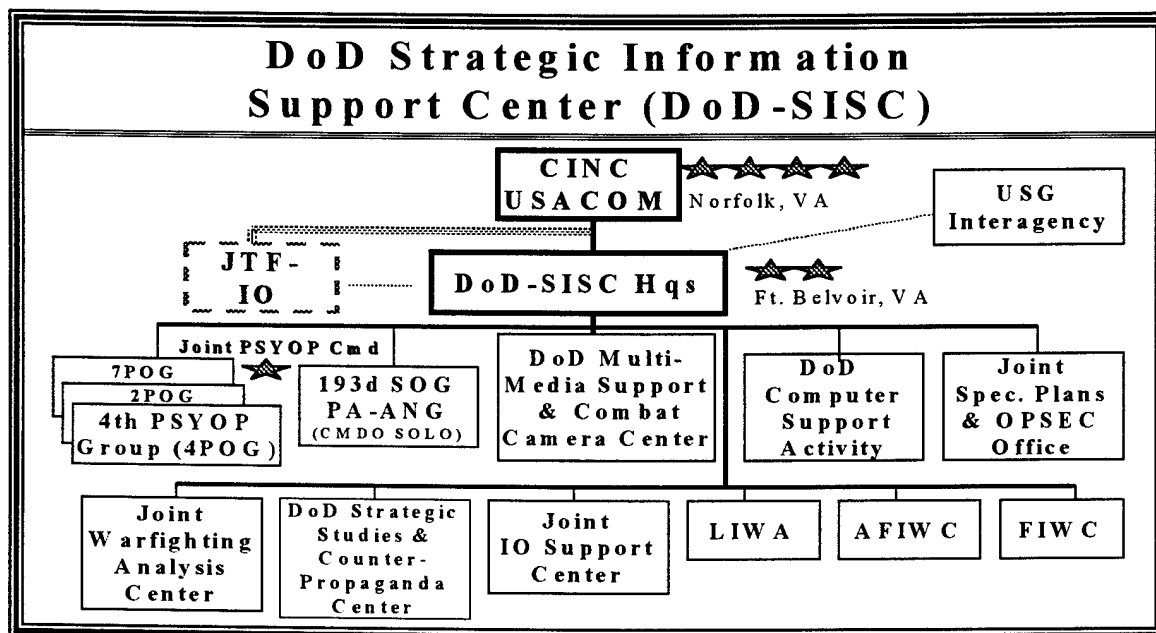


Figure 3. Recommend Organizational Structure  
Headquarters Section

Creating a sub-unified command under Atlantic Command (USACOM) is a logical choice for a number of reasons. First, USACOM is the joint force provider and integrator, and joint doctrine proponent. Second, it has a staff that routinely conducts coordination with the interagency. Third, it is physically the closest Commander-in-Chief to Washington, DC which facilitates face-to-face interagency coordination.<sup>46</sup> Fourth, it currently has several joint commands, two of which are the Joint Command and Control Warfare Center and the Joint Warfighting Analysis Center.

As the joint force integrator, USACOM synergistically blends "technology, systems, and doctrine from the different military departments. This integration will

improve interoperability, and enhance joint force capabilities.”<sup>47</sup> Upon approval of the Presidential Decision Directive on International Public Information (PDD-IPI), a document “intended to coordinate the U.S. government’s numerous public relations offices . . . to counter future barrages of hate propaganda anywhere in the world” will create two new posts at the State Department—an Undersecretary of State for Public Diplomacy and a Senior Coordinator for International Public Information.<sup>48</sup> The DoD Strategic Information Support Center would be a U.S. military link into the interagency process in accordance with the Presidential Decision Directive on International Public Information.<sup>49</sup>

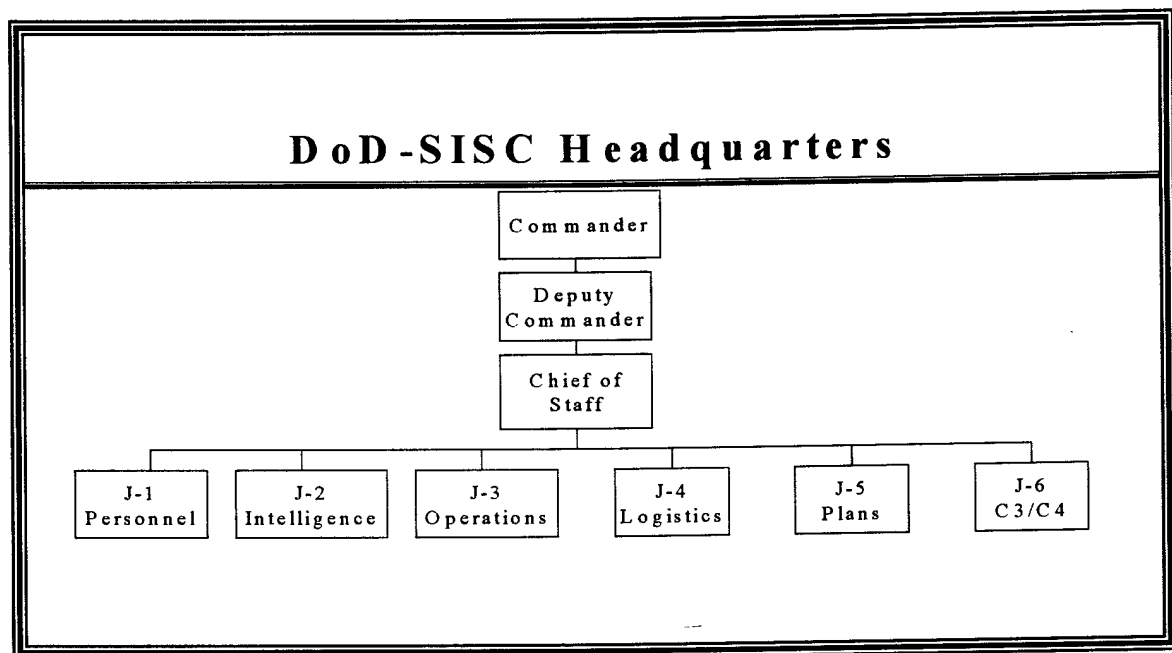


Figure 4. DoD-SISC Headquarters

The Defense Information Support Activity (DISA) would provide all communications support to the headquarters. This two-star headquarters would have operational control of all assigned units. Figure 4 depicts the headquarters and staff of the DoD-SISC. The staff would be lean and leverage current organizations to provide

support. For example, the J2, intelligence, section would leverage existing capabilities currently available at the Defense Intelligence Agency and subordinate units' intelligence and information collection capability, such as those found in the Joint Information Operations Support Center (formerly the JC2WC) and combat camera units. The J4, logistics, section would coordinate logistics for the joint commander. Logistics is a Service responsibility so the DoD-SISC would coordinate with the Services to ensure his commander's needs were considered. The J6, command, control, communications, and computers (C<sup>4</sup>), section would maintain the C<sup>4</sup> architecture for the Center in coordination with the Defense Information Support Activity.

#### Joint Task Force-Information Operations

At the direction of the Secretary of Defense, the DoD-SISC could establish a Joint Task Force for Information Operations (JTF-IO) responsible for military information activities for an operation. This joint task force would be comprised of subordinate units to meet the needs of the supported Commander-in-Chief. For example, U.S. European Command (USEUCOM) would receive a JTF-IO comprised of elements from the Joint Psychological Operations Command, Computer Network Defense Activity, Joint Information Operations Support Center, and Service Information Operations organizations. This JTF would provide information operations support to the supported Commander-in-Chief and subordinate component commanders. It would have a reach-back capability to the DoD-SISC's Multi-media Support Center, Strategic Studies and Counter-Propaganda Center, and the Joint Warfighting Analysis Center. Pooling requirements for expensive satellite time and buying blocks of time well into the future will save the U.S. government significant sums of money.

### Joint Psychological Operations Center

The Joint Psychological Operations Center, a one-star psychological operations command, also to be located at Fort Belvoir, Virginia would conduct tactical, operational, and strategic psychological operations.<sup>50</sup> Current psychological operations forces would be reconfigured to make best use of this asset. Some production members from the print and audio/visual units would move to the DoD Multi-media Support Center.

#### Strategic Studies, Counter-Deception, Special Plans and Operations Security

Some civilian members of the 4<sup>th</sup> Psychological Operations Group's Strategic Studies Detachment would create the DoD Strategic Studies and Counter-Propaganda Center with members from the Defense Intelligence Agency's Human Factors Analysis Center and the Detection of Foreign Deception office.

Members, staffs, and organizations of the Armed Forces with deception planning expertise would comprise the Joint Special Plans and Operations Security Office.

#### Multi-Media Support and Combat Camera Center

Production resources and dissemination assets from the 4<sup>th</sup> Psychological Operations Group, Joint and Service combat camera units, and the Armed Forces Radio and Television Service (AFRTS) would compose the Multi-Media Support and Combat Camera Center. Some of the capabilities of these organizations are duplicative, such as television and radio production and dissemination capabilities. The Center could pool equipment, modernize equipment, and leverage the technical expertise currently dispersed among numerous disjointed organizations.

The Center would have world-class radio and television production and dissemination facilities that would rival Cable News Network's capabilities. The Center



would perform the archival functions currently performed by the Joint Combat Camera Center and the Defense Visual Information Center. The archived footage would be shared by all information activities. Both public affairs and psychological operations units could still maintain autonomy while executing operations, however, they could share expensive, highly technical production assets.

#### DoD Computer Support Activity

The Computer Support Activity would incorporate all Department of Defense organizations currently performing or possessing the capability to conduct computer network attack, computer network defend, and computer emergency response team operations.<sup>51</sup> Currently, the Joint community and the Services each have their own computer network defend and computer emergency response team organizations. Additionally, there are regional Service computer emergency response teams performing those same functions. By combining these organizations, their expertise could be leveraged to the benefit of the Armed Forces. The Services would still receive support, however, the administrative overhead required to man, maintain, and sustain an organization could be streamlined.<sup>52</sup>

#### Modeling and Simulation

The Joint Warfighting Analysis Center (JWAC), a subordinate unit of U.S. Atlantic Command, would provide modeling and simulation support to the DoD Strategic Information Support Center. It would be the Armed Forces central modeling and simulations organization for information operations. It would receive personnel and equipment involved in modeling and simulations from the Joint and Service information operations organizations. The Center would harness the technical expertise currently

scattered among several organizations that perform similar modeling and simulations functions. The synergistic benefits gained by grouping these experts under one organization far outweighs any costs associated with moving equipment and personnel. In most cases, the people and equipment would remain in their current location, however, they would respond to one organization with the responsibility to perform modeling and simulations functions.

### Joint and Service Information Operations Centers

Aside from moving some personnel out of the joint and Service information operations centers to other organizations within the DoD Strategic Information Support Center, they would remain the same. In some cases, the Commanders-in-Chief and Service Components would receive the support previously provided by the joint and Service information operations centers, but from a different organization. For example, the Services would receive computer network defense support from the Computer Support Activity instead of their individual Computer Emergency Response Teams. Similarly, the Joint Warfighting Analysis Center would provide modeling and simulation support instead of each Service information operations center.

### Evaluation

This monograph uses several evaluation criteria to evaluate how a DoD Strategic Information Support Center can meet the needs of the Armed Forces in the 21<sup>st</sup> Century. These criteria are integration, speed, flexibility, and synergy. **Joint/Interagency integration** is defined as an organization in which elements of more than one Service participates and conducts liaison with other organizations of the U.S. Government. **Speed** is defined as less 'startup' time between deployment and employment than the

current organizational structure allows. **Organizational flexibility** is defined as the ability to offer numerous and multi-functional force packages to meet the informational needs of the supported commander. **Synergy** is defined as achieving greater results than the sum benefits or at less cost than those benefits or costs of the composite organizations.

As stated previously, there is no one military organization responsible for information activities. Additionally, there is no single staff to which the U.S. Government Interagency can turn to receive information on policy, doctrine, or current military operations as related to information activities. Three Assistant Secretaries of Defense and two Commanders-in-Chief have responsibility for the disparate military information activities. The DoD Strategic Information Support Center would provide one organization to which the Interagency could coordinate, integrate, deconflict, and synchronize U.S. Government strategic information activities with military information activities.

This lack of unity at the highest level impedes the speed at which Commanders-in-Chief and component commanders receive support from military organizations involved in the planning, conduct, or assessment of information activities. Additionally, there is much confusion within the military as to the relationship among these various organizations. For example, during operations in Bosnia, a Division commander tasked the Land Information Warfare Activity to develop and disseminate psychological operations products. The Activity has neither the charter nor the expertise to accomplish that mission. As desktop publishing and access to national level intelligence becomes more readily available, a danger exists that untrained individuals will attempt to

accomplish a mission for which they are untrained. Similarly, the current archaic approval process used for psychological operations is a prime example of the timeliness problem. During Operation Desert Shield/Storm, the approval process took over four months. The Armed Forces must be capable of rapidly responding to the information needs of its commanders. An organization such as the DoD Strategic Information Support Center would rapidly tailor support to meet the needs of warfighting commanders.

The supported commander would state his requirements in the form of missions and the DoD Strategic Information Support Center would tailor packages to meet those requirements. For example, it would build a Joint Task Force for Information Operations (JTF-IO) composed of personnel from its subordinate organizations to meet the needs of the supported commander. The Commander, JTF-IO would be responsible for coordinating, integrating, deconflicting, and synchronizing the operations of the JTF in accordance with both the Theater Information Strategy and U.S. Government strategic information activities.

Currently there is a dearth of experience in the art and science of persuasive communications, computer network defense operations, and technical analysis resident in the U.S. military. It must harness the expertise it has within several disparate organizations to achieve synergy. The Joint Special Operations Command, a subordinate command of U.S. Special Operations Command, sets the precedent for this type of organization. One in which highly-specialized experts are resident in one organization and are available to Commanders-in-Chief within a short time frame.

## Conclusions

In an environment of shrinking budgets, increased operational tempo, and continued downsizing, the U.S. Armed Forces must change the way it is organized, trained, and equipped to meet the needs of the 21<sup>st</sup> Century and *Joint Vision 2010*. Recent history demonstrates that the side with the ability to rapidly present its policy, strategy, and position to a variety of audiences in a coherent manner achieves an information advantage. The U.S. Government recognizes this fact and is taking steps to “leverage information to prevent or mitigate foreign crises and to promote policies in the global information environment.”<sup>53</sup> The military must also adapt to this changing global information environment. A single organization, such as the DoD Strategic Information Support Center, from which military information activities can be coordinated, integrated, deconflicted, and synchronized is a step in the right direction.

## ENDNOTES

<sup>1</sup> "Jackson meets with POWs during intense day of bombing," *Kansas City Star*, 1 May 1999, A-12.

<sup>2</sup> Matthew Kaminski, "Propaganda Push by NATO Gets Slow Start," *Wall Street Journal*, April 20, 1999, 19. Also see, Kenneth Allard, "War by other means: Milosevic beats Clinton at his own game: TV," at <http://www.msnbc.com/news/265101.asp> accessed 4 May 1999. Dr. Allard is a senior associate at the Center for Strategic & International Studies and an MSNBC military analyst.

<sup>3</sup> Massimo Calabresi, "Mind Games," *Time*, May 3, 1999, 60.

<sup>4</sup> Anthony Lewis, "Mr. Milosevic's Campaign of Terror," *The New York Times*, March 27, 1999 at <http://www.nytimes.com/library/opinion/lewis/032799lewi.html> accessed 4 May 99. See also, Howard Kurtz, "U.S. Tack: Demonize Enemy, Tightly Control Information," *Washington Post*, March 27, 1999, 13.

<sup>5</sup> Justin Brown, "Why Serb Chief Whips Up Anti-US Fervor," *Christian Science Monitor*, April 1, 1999, at <http://www.csmonitor.com/durable/1999/04/01/fp11s3-csm-shtml>.

<sup>6</sup> Alex Todorovic, "I'm Watching Two Different Wars," *Washington Post*, April 18, 1999, B1.

<sup>7</sup> *Meet The Press*, host Tim Russert, NBC, 2 May 2, 1999. Tim Russert asked Secretary of Defense William Cohen and Joint Chiefs of Staff Vice-Chairman General Ralston "But a selective air campaign, without the threat of ground forces—when has that ever worked?"

<sup>8</sup> Bradley Graham, "Analysis: Warnings Of Air War Drawbacks," *Washington Post*, April 27, 1999, 1.

<sup>9</sup> John Keegan, "Why NATO Was Determined To Wage War From The Air Alone," *London Daily Telegraph*, April 15, 1999 cited in the *Earlybird*, 15 April 1999.

<sup>10</sup> Philip Handleman, "U.S. Can Still Win War Without Ground Troops," *Detroit News*, May 3, 1999, 7.

<sup>11</sup> Stephen S. Rosenfeld, "In the Seventh Year," *Washington Post*, April 23, 1999, 37.

<sup>12</sup> Michael D. Furlong, Lieutenant Colonel, U.S. Army, Retired, former commander of the 6<sup>th</sup> PSYOP Bn (A). Interview with author February 1999.

---

<sup>13</sup> Office of Coordination of Information (1941), the Office of Strategic Services (1942), State-War-Navy Coordinating Committee (1946), Psychological Warfare Strategy Board (1951), PSYOP Coordinating Committee (1986) are a few examples of organizations with the charter to coordinate and develop U.S. government information activities.

<sup>14</sup> IPI Framework Document, draft, dated April 6, 1998.

<sup>15</sup> Currently there is a Presidential Decision Directive on International Public Information (PDD-IPI) pending approval. This PDD would update NSDD 130 for the 21<sup>st</sup> Century.

<sup>16</sup> LTC (Ret) Michael D. Furlong. The U.S. government Deputies' Committee approved this name change in November 1998.

<sup>17</sup> Joint Chiefs of Staff, Joint Publication 3-13, *Joint Doctrine for Information Operations* (Washington, DC: 9 October 1998), I-9.

<sup>18</sup> *Joint Vision 2010*, 28-29.

<sup>19</sup> *Joint Vision 2010*, 31.

<sup>20</sup> LTC (Ret) Michael D. Furlong.

<sup>21</sup> For example, the 300<sup>th</sup> Military Intelligence Brigade uses derivative Unit Identification Codes (UICs) to activate and deploy small teams instead of activating an entire unit.

<sup>22</sup> BBC Online Network, "Demonstrators call for holy war," August 21, 1998 and "Osama bin Laden 'innocent'," November 21, 1998 at [http://news.bbc.co.uk/hi/english/world/newsid\\_155000/155917.stm](http://news.bbc.co.uk/hi/english/world/newsid_155000/155917.stm) accessed 17 and 15 April 1999.

<sup>23</sup> Robert W. Noonan, Jr. Major General, Commanding General, U.S. Intelligence and Security Command. United States Army Intelligence presentation to Brigade and Battalion Pre-Command Course 99-07 on 14 April 1999 at Fort Leavenworth, KS.

<sup>24</sup> Elizabeth de Bony, "NATO Reinforces Against Net Attack From Serbs," article at [www.infowar.com](http://www.infowar.com) accessed 15 April 1999.

<sup>25</sup> These statements are in response to the NATO bombing of civilian vehicles in a convoy in Yugoslavia in April 1999. Rick Montgomery, "Modems, motives give us Web War I," *Kansas City Star*, 18 April 1999, A-1 & A-16.

---

<sup>26</sup> *Joint Vision 2010*, p. 8-9.

<sup>27</sup> LTC (Ret) Michael D. Furlong.

<sup>28</sup> Ralph Peters, "How Saddam Won This Round," *Newsweek*, November 30, 1998, Vol 132 Issue 22, p. 39.

<sup>29</sup> Joint Command and Control Warfare Center homepage at <http://www.aia.af.mil/common/homepages/pa/bios/jc2wc.htm> accessed 1 April 1999.

<sup>30</sup> Joint Command and Control Warfare Center (JC2WC) Command Brief provided by Trenton Lennard, Lieutenant, U.S. Navy, JC2WC.

<sup>31</sup> Land Information Warfare Activity, *Field Support Team CD*, unclassified edition (Ft Belvoir, VA: 29 September 1998).

<sup>32</sup> Unfortunately, the LIWA does not have sufficient subject matter expertise in some critical areas, such as psychological operations. To fill that gap LIWA sends its FST members to a psychological operations course conducted at either Ft Bragg, NC or Hurlbert Field, FL.

<sup>33</sup> Patrick Scribner, Major, U.S. Army, Land Information Warfare Activity, Field Support Team Leader, interview with author, 7 April 1999.

<sup>34</sup> *Field Support Team CD*.

<sup>35</sup> Russell Brune, Lieutenant, U.S. Navy, Fleet Information Warfare Center, interviews with author, April 1999.

<sup>36</sup> The TAMT-10, operated by the 4<sup>th</sup> Psychological Operations Group (Airborne), is capable of radio transmission, reception, and production. It broadcasts from 535-1705KHz; range is 80km. Commando Solo, operated by the 193d Special Operations Squadron, Pennsylvania Air National Guard, is an airborne electronic broadcasting platform capable of broadcasting AM/FM radio, television, short-wave and military communication bands.

<sup>37</sup> Air Force Information Warfare Center homepage at <http://www.aia.af.mil/common/homepages/pa/bios/iwcfact.html> accessed 1 April 1999.

<sup>38</sup> U.S. Air Force Publication 2-5 (AFDD 2-5), *Information Operations*, accessed at <http://www.doctrine.af.mil/main.asp>, on 15 April 1999.

<sup>39</sup> A more detailed description would be beyond the classification of this monograph. The reader should be aware that assets are available for deception planning and execution.



---

<sup>40</sup> Douglas Waller, "How a Spec Ops Campaign Saved Lives," *Armed Forces Journal International* (June 1995), 35.

<sup>41</sup> A re-evaluation of PSYOP's command relationships is needed to determine the optimal. Due to the overriding requirements of USSOCOM's Joint Special Operations Command and the institutional bias favoring Special Forces units, the PSYOP unit's priorities pale in comparison. The 1997-2002 Program Objective Memorandums support this assertion that PSYOP have low priority for funding within USSOCOM.

<sup>42</sup> 690<sup>th</sup> IOS homepage at <http://www.ioc.aia.ic.gov> accessed on 14 April 1999.

<sup>43</sup> Jeff Elliott, Lieutenant, U.S. Navy, Officer in Charge, Joint Combat Camera Center, interview with author on 7 April 1999; Worldwide DOD Visual Information and Combat Camera Conference and Workshop (DEC 1-4) Compact Disk, provided by LT Elliott; and Joint Combat Camera Center homepage at <http://dodimagery.afis.osd.mil/about.html> accessed 5 April 1999.

<sup>44</sup> Everette E. Dennis, and others. *The Media at War: The Press and the Persian Gulf Conflict* (New York City: Freedom Forum Media Studies Center, June 1991), 86.

<sup>45</sup> DoDD S-3321.1 (PSYOP), DoDD 3600.1 (IO), several DoDDs for PA. In fact, the public affairs discipline has twelve different DoDDs covering fragments of that arena.

<sup>46</sup> Regardless of current technology, the majority of interagency coordination occurs face-to-face not via video teleconferencing or other technical means.

<sup>47</sup> USACOM homepage at [http://www.acom.mil/acomweb.nsf\\*/AboutUSACOM](http://www.acom.mil/acomweb.nsf*/AboutUSACOM), accessed 5 April 1999.

<sup>48</sup> Neil Munro, "Inducting Information," *National Journal* 27 March 1999 at [http://www.infowar.com/mil\\_c4i\\_032999c\\_j.shtml](http://www.infowar.com/mil_c4i_032999c_j.shtml), accessed on 1 April 1999 and Lieutenant Colonel Michael D. Furlong.

<sup>49</sup> Research sponsored by ASD(SOLIC) revealed that acute manpower shortages within the U.S. Government Interagency are a key deficiency that hinders optimal performance for U.S. Government strategic information activities. Pooling resources within the DoD-SISC is an option for improving the utilization of the scarce manpower currently available. The OASD(SOLIC) and the Joint Staff (J-39) have representatives on the IPI Core Group's Interagency Working Group. The DoD-SISC will provide the depth to the DoD IPI effort that currently does not exist. One GS-15 within OASD(SOLIC) is the only full-time IPI and PSYOP support. The Joint Staff has four officers assigned to PSYOP; however, this office has a portfolio ranging from IPI Core Group activities, to doctrine, training, deployment orders, plans, and information

---

operations. These primary players need a depth of surge support behind them to be effective. The concept of the DoD-SISC is to pool resources from several agencies and organizations so that there is a one-stop shop for strategic and operational information support.

<sup>50</sup> This organization currently does not exist, but USSOCOM in accordance with the 1990 Master PSYOP Plan is readdressing the issue of PSYOP's command relationship.

<sup>51</sup> For classification purposes, this monograph will not address CNA operations.

<sup>52</sup> The expertise required to conduct CND and CERT operations is highly technical. While there are qualified individuals serving in the Armed Forces who conduct these operations, their long-term retention in the military is questionable.

<sup>53</sup> IPI Framework Document (Draft), 1.

## BIBLIOGRAPHY

### Articles

- Calabresi, Massimo. "Mind Games." *Time*, May 3, 1999, 60.
- Gough, Patrick, Major, USMC. "The Joint Command and Control Warfare Center Command Information." *Cyber Sword: The Professional Journal of Joint Information Operations*, Vol 1, No. 1 (Spring 1997), 6-9.
- Graham, Bradley. "Analysis: Warnings Of Air War Drawbacks." *Washington Post*, April 27, 1999, 1.
- Handleman, Philip. "U.S. Can Still Win War Without Ground Troops." *Detroit News*, May 3, 1999, 7.
- Kaminski, Matthew. "Propaganda Push by NATO Gets Slow Start." *Wall Street Journal*, April 20, 1999, 19.
- Keegan, John. "Why NATO Was Determined To Wage War From The Air Alone." *London Daily Telegraph*, April 15, 1999 cited in the *Earlybird*, 15 April 1999.
- Kurtz, Howard. "U.S. Tack: Demonize Enemy, Tightly Control Information." *Washington Post*, March 27, 1999, 13.
- Montgomery, Rick. "Modems, motives give us Web War I." *Kansas City Star*, 18 April 1999.
- Peters, Ralph. "How Saddam Won This Round." *Newsweek*, November 30, 1998, Vol 132, Issue 22, 39.
- Rosenfeld, Stephen S. "In the Seventh Year." *Washington Post*, April 23, 1999, 37.
- Swart, William R. "Modeling & Simulation: Essential Ingredient for Successful Information Operations." *Cyber Sword: The Professional Journal of Joint Information Operations*, Vol 2, No. 1 (Spring 1998), 18-19.
- Thomas, Timothy L. "The Age of the New Persuaders." *Military Review* (May-June 1997): 72-80.
- Todorovic, Alex. "I'm Watching Two Different Wars." *Washington Post*, April 18, 1999, B1.
- Tolbert, Don, Major. "Introduction to JC2WC Software Support." *Cyber Sword: The Professional Journal of Joint Information Operations*, Vol 1, No. 2 (Fall 1997), 10-12.

Waller, Douglas. "How a Spec Ops Campaign Saved Lives." *Armed Forces Journal International* (June 1995), 35.

Wilson, George C. "Losing the War of Words." *Washington Post*, March 30, 1998, A25.

### **Books**

Dennis, Everette E. and others. *The Media at War: The Press and the Persian Gulf Conflict*. New York City: Freedom Forum Media Studies Center, June 1991.

Siegel, P.C. *Target Bosnia: Integrating Information Activities in Peace Operations*. Fort McNair: National Defense University Press, 1998.

### **Electronic Sources**

Air Force Information Warfare Center homepage accessed at  
<http://www.aia.af.mil/common/homepages/pa/bios/iwcfact.html> on 1 April 1999.

Allard, Kenneth. "War by other means: Milosevic beats Clinton at his own game: TV." Accessed at <http://www.msnbc.com/news/265101.asp> on 4 May 1999.

BBC Online Network, "Demonstrators call for holy war." 21 August 1998. "Osama bin Laden 'innocent'." 21 November 1998. Accessed at  
[http://news.bbc.co.uk/hi/english/world/newsid\\_155000/155917.stm](http://news.bbc.co.uk/hi/english/world/newsid_155000/155917.stm) on 17 and 15 April 1999.

Brown, Justin. "Why Serb Chief Whips Up Anti-US Fervor." *Christian Science Monitor*, April 1, 1999. Accessed at  
<http://www.csmonitor.com/durable/1999/04/01/fpl1s3-csm-shtml> on 15 April 1999.

de Bony, Elizabeth. "NATO Reinforces Against Net Attack From Serbs." *InfoWorld Electric*, April 10, 1999. Accessed at <http://www.infowar.com> on 15 April 1999.

Joint Combat Camera Center homepage accessed at  
<http://dodimagery.afis.osd.mil/about.html> on 5 April 1999.

Joint Command and Control Warfare Center homepage accessed at  
<http://www.aia.af.mil/common/homepages/pa/bios/jc2wc.htm> on 1 April 1999.

Lewis, Anthony. "Mr. Milosevic's Campaign of Terror." *The New York Times*, March 27, 1999 accessed at  
<http://www.nytimes.com/library/opinion/lewis/032799lewi.html> on 4 May 99.

Munro, Neil. "Inducting Information." *National Journal*, 27 March 1999 accessed at [http://www.infowar.com/mil\\_c4i\\_032999c\\_j.shtml](http://www.infowar.com/mil_c4i_032999c_j.shtml) on 1 April 1999.

U.S. Army Land Information Warfare Activity (LIWA). *LIWA Field Support Team (FST) Compact Disk, Unclassified Edition*. Fort Belvoir, VA: USAINSCOM. 29 SEP 98.

U.S. Atlantic Command homepage accessed at [http://www.acom.mil/acomweb.nsf/\\*/AboutUSACOM](http://www.acom.mil/acomweb.nsf/*/AboutUSACOM) on 5 April 1999.

U.S. Department of the Air Force. AFDD 2-5. *Information Operations*. Accessed at <http://www.doctrine.af.mil/main.asp> on 15 April 1999.

U.S. Department of Defense. *The Joint Doctrine Encyclopedia* [online edition]; available from <http://www.dtic.mil/doctrine/jrm/ency.htm> on Intellink.

300<sup>th</sup> Military Intelligence Brigade command brief provided by Major Barbara J. Hirst.

690<sup>th</sup> IOS homepage at <http://www.ioc.aia.ic.gov> accessed on 14 April 1999.

### Government Documents

Armed Forces Staff College (AFSC). AFSC Pub 12. *Joint Information Warfare Staff Officer's Guide*. Norfolk, VA: AFSC, February 1998.

\_\_\_\_\_. *Joint Information Operations Planning Handbook. Preliminary Draft*. Norfolk, VA: AFSC, nd.

Chairman of the Joint Chiefs of Staff. *Joint Vision 2010*.

Noonan, Robert W. Jr. Major General. Commanding General, U.S. Intelligence and Security Command. United States Army Intelligence presentation to Brigade and Battalion Pre-Command Course 99-07 on 14 April 1999 at Fort Leavenworth, KS.

U.S. Department of the Army. FM 33-1-1. *Psychological Operations Techniques and Procedures*. Washington, DC: Government Printing Office, 5 May 1994.

\_\_\_\_\_. FM 100-6. *Information Operations*. Washington, DC: Government Printing Office, 27 August 1996.

U.S. Department of Defense. Joint Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office, 23 March 1994.

- \_\_\_\_\_. Joint Pub 3-0. *Doctrine for Joint Operations*. Washington, DC: Government Printing Office, 1 February 1995.
- \_\_\_\_\_. Joint Pub 3-13. *Joint Doctrine for Information Operations*. Washington, DC: Government Printing Office, 9 October 1998.
- \_\_\_\_\_. Joint Pub 3-13.1. *Joint Doctrine for Command and Control Warfare (C2W)*. Washington, DC: Government Printing Office, 7 February 1996.
- \_\_\_\_\_. Joint Pub 3-61. *Doctrine for Public Affairs in Joint Operations*. Washington, DC: Government Printing Office, 14 May 1997.

*International Public Information Framework Document Draft*. 6 April 1998. Received from member of the Joint Staff.

### **Interviews**

- Brune, Russell. Lieutenant, U.S. Navy, Fleet Information Warfare Center. Several interviews with author, March-April 1999.
- Caruso, Mark A. Major, U.S. Army, Plans, Programs, Doctrine, Force Integration and Development, 4<sup>th</sup> Psychological Operations Group (Airborne). Interview with author December 1998.
- Castillo, David. Lieutenant Colonel, U.S. Air Force, Commander, 690th Information Operations Squadron. Interview with author March 1999.
- Elliott, Jeff. Lieutenant, U.S. Navy, Joint Combat Camera Center. Interview with author, 7 April 1999.
- Furlong, Michael D. Lieutenant Colonel (Retired), U.S. Army. Numerous interviews and email discussions with author, February - April 1999.
- Lennard, Trenton. Lieutenant, U.S. Navy, Joint Command and Control Warfare Center. Interview with author, March 1999.
- Markham, John. Lieutenant Colonel, U.S. Army, Joint Command and Control Warfare Center. Interview with author, March 1999.
- Scribner, Patrick. Major, U.S. Army, Land Information Warfare Activity. Interview with author 7 April 1999.
- Trost, Robert. Colonel (Retired), U.S. Army, The Joint Staff, Pentagon. Interview with author 18 February 1999.

### **Monographs and Theses**

Doyle, Kevin J. "Information Operations: A Look at Emerging Army Doctrine and its Operational Implications." MMAS monograph, School of Advanced Military Studies, Fort Leavenworth, 1995.

Lane, Randall C. "Information Operations: A Joint Perspective." MMAS monograph, School of Advanced Military Studies, Fort Leavenworth, 1998.

Straughan, Matt. "Information Operations and Unity of Effort." Paper, Naval War College, Newport, RI, 13 June 1997.